Application Number 09/900,496
Responsive to Office Action mailed August 17, 2005

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

Claim 1 (Currently Amended): A method for secure communications between a client and one of a plurality of servers performed on an intermediary device coupled to the client and said plurality of servers, comprising:

(a) establishing an open communications session between the intermediary device and the client via an open network;

(b) negotiating a secure communications session with the client;

(c) establishing an open communications session with said one of said plurality of servers via a secure network;

(d) receiving encrypted application data from the client via the secure communications session;

(e) decrypting the encrypted applications data;

(f) forwarding the decrypted application data to the server via the secure network;

(g) receiving application data from the server via the secure network;

(h) encrypting the application data; and

(i) sending encrypted application data to the client,

wherein the steps (e) and (f) are performed at the packet level of a network stack of the intermediate device without processing the application data with an application layer of a network stack.

Claim 2 (Original): The method of claim 1 wherein said step (a) comprises the sub steps of:

receiving a request for a communications session from the client;

responding to the request for a communications session in place of the server; and

establishing a secure communications session between the client and the intermediary device.

Claim 3 (Original): The method of claim 2 wherein said step of (a) comprises receiving a TCP SYN packet from a client and responding to the SYN packet with appropriate responses as a proxy for the server.

Claim 4 (Original): The method of claim 1 wherein said step of negotiating a secure communications session comprises negotiating an SSL session with the client in place of the server.

Claim 5 (Currently Amended): The method of claim 1 further including:

receiving the application data as multi-segment records;

forwarding at least a portion of the decrypted application for each of the records prior to receiving complete records;

discarding ~~at least a~~ the portion of each of the records after forwarding the portion to be discarded; and

authenticating the decrypted application data of each data record using the remaining non-discarded portion of the data record upon receiving a final segment of the multi-segment record.

Claim 6 (Original): The method of claim 1 wherein the step of forwarding decrypted application data to said one of said plurality of servers comprises forwarding authenticated application data.

Claim 7 (Previously Presented): The method of claim 6 wherein said step of forwarding unauthenticated application data includes the further, subsequent step of authenticating the data.

Claim 8 (Previously Presented): The method of claim 1 wherein, prior to said step of establishing a communications session with one of said plurality of servers, the method includes the step of:

selecting one of said plurality of servers to forward said decrypted authentication data to based on a load balancing algorithm that calculates current processing loads associated with each of the servers.

Claim 9 (Original): The method of claim 8 further including the step of:

tracking data passing between the client and said one of said plurality of servers.

Claim 10 (Original): The method of claim 9 wherein said step of tracking comprises:

establishing a session tracking database recording, for each session, a session ID, a TCP sequence number and an SSL session number.

Claim 11 (Original): The method of claim 10 further including tracking, for each session, an initialization vector.

Claim 12 (Previously Presented): An apparatus coupled to a public network and a secure network, communicating with at least one client via the public network and communicating with one of a plurality of servers via the secure network, comprising:

a network interface communicating with the public network and the secure network;

at least one processor;

programmable dynamic memory addressable by the processor;

a communications channel coupling the processor, memory and network communications interface;

a proxy TCP communications engine;

a proxy SSL communications engine;

a server TCP communications engine; and

a packet data encryption and decryption engine,

wherein the proxy SSL communications engine and the server TCP communications engine decrypt encrypted application data from the client and forward the decrypted application data to the one of the plurality of servers without processing the application data with an application layer of a network stack of the apparatus.

Claim 13 (Previously Presented): The apparatus of claim 12 further comprising a negotiation manager that enables the apparatus as a TCP and SSL proxy for the server.

Claim 14 (Original): The apparatus of claim 12 further including a load balancing engine to direct application data between the at least one client and said one of said plurality of servers by copying the data from an SSL communications session established by the SSL communications engine to a server TCP session established by the server TCP communications engine.

Claim 15 (Original): The apparatus of claim 12 wherein the encryption and decryption engine decrypts encrypted packet data to produce application data.

Claim 16 (Original): The apparatus of claim 12 further including a session tracking database having at least one record per communication session between the client and server.

Claim 17 (Original): The apparatus of claim 16 wherein said at least one record includes a TCP sequence number and an SSL sequence number.

Claim 18 (Original): The apparatus of claim 16 further including a recovery manager using said database to recover from communication errors.

Claim 19 (Original): The apparatus of claim 12 wherein the packet data encryption and decryption engine decrypts packets from SSL data which spans over multiple TCP segments and forwards packet data to a server which is not authenticated.

Claim 20 (Previously Presented): The apparatus of claim 12 wherein said data is not buffered during decryption.

Claim 21 (Previously Presented): The apparatus of claim 12 wherein said data is buffered for a length sufficient to complete a block cipher used to encrypt the data.

Claim 22 (Currently Amended): The apparatus of claim 19,

wherein said packet data encryption and decryption engine includes an authentication process which authenticates the decrypted data after a final segment of a multi-segment encrypted data record is received, and

wherein the authentication process discards at least a portion of the data record after forwarding the portion to be discarded and authenticates decrypted data using the remaining portion of the data record after the final segment is received.

Claim 23 (Currently Amended): A method of providing secure communications between a plurality of customer devices and an enterprise, comprising:

providing a device enabled for secure communication with customer devices and having an IP address of the enterprise;

receiving with an intermediate device communications directed to the enterprise in secure protocol, wherein the secure protocol provides encrypted application data associated with an application layer of a network stack;

decrypting data packets of the secure protocol to provide decrypted packet data at the packet-level of a network stack of the intermediate device;

bypassing the ~~an~~ application layer of the network stack of the intermediate device and forwarding the decrypted packet data from the intermediate device to at least one server of the enterprise without processing the decrypted packet data with the application layer;

receiving application data from a secure server of the enterprise;

encrypting the application data received from the enterprise; and

forwarding encrypted application data to the customer.

Claim 24 (Original): The method of claim 23 wherein the secure communication in SSL protocol encrypted application data.

Claim 25 (Original): The method of claim 23 wherein said step of receiving comprises the sub steps of initiating a communication session with the enterprise and negotiating a secure communication session with the device.

Claim 26 (Original): The method of claim 23 further including the step of negotiating an open communications session with said at least one server of the enterprise and wherein said step of forwarding includes forwarding decrypted data via the open communications session.

Claim 27 (Original): The method of claim 23 wherein said step of receiving communications includes receiving a plurality of secure communications sessions from a plurality of customers.

Claim 28 (Original): The method of claim 27 further including a step of selecting one of a plurality of enterprise servers to which to direct data in said step of forwarding said decrypted packet data.

Claim 29 (Original): The method of claim 28 further including the step of tracking each communications session between each of said plurality of customers and an associated one of said plurality of enterprise servers.

Claim 30 (Currently Amended): A method for secure communications between a client and one of a plurality of servers performed on an intermediary device coupled to the client and said plurality of servers, comprising:

(a) establishing an open communications session between the intermediary device and the client device via an open network;

(b) negotiating a secure communications session between the intermediary device and the client;

(c) establishing an open communications session between the intermediary device and said one of said plurality of servers via a secure network;

(d) receiving encrypted application data from the client via the secure communications session;

(e) decrypting the encrypted application data;

(f) bypassing an application layer of a network stack of the intermediate device and forwarding the decrypted application data from the intermediate device to the server via the secure network without processing the decrypted ~~packet~~ application data with the application layer;

(g) receiving application data from the server via the secure network;

(h) encrypting the application data;

(i) sending encrypted application data to the client;

(j) detecting a communications anomaly in a communications session between the client and the intermediary device; and

(k) passing TCP data between the client and the server ~~from~~ through the intermediary device.